REMARKS

The specification has been amended to make editorial changes therein.

Independent claims 1, 22-23 and 31 have been amended and claims 7 and 38 have been canceled. Claim 20 has been amended to depend from claim 1. All of the other dependent claims have been amended to place them in a form more suited to U.S. practice and into conformance with the amended independent claims.

Claim 38 was rejected under §112, second paragraph. Withdrawal of the rejection is respectfully requested.

Claims 1-38 were rejected as anticipated by CHEFALAS et al. 2002/0116639. Reconsideration and withdrawal of the rejection of claims 1-6 and 8-37 are respectfully requested.

Claims 1, 22-23, and 31 have been amended to provide that one or more predetermined actions are performed to activate unknown viruses and to detect the activated unknown viruses by detecting consequences of virus activation. Support for this amendment is found on page 12, line 32. CHEFALAS et al. do not disclose taking actions to activate unknown viruses (it only deals with known viruses) or detecting the consequences of activation of unknown viruses, and the amended claims avoid the rejection under §102.

By way of further explanation, CHEFALAS et al. disclose a solution for virus detection and elimination, wherein client

devices 110-118 locally monitor the presence of known viruses and notify a server 106 whenever one is detected. The server 106 may further inform the remote administrator 138 and take actions such as severing the communication link to the client(s) 110-118 sending the notification(s). Notifications may include identification of the detected virus.

However, in the claimed invention, a security system comprises a first sub-system that is set up for deliberately activating unknown viruses in a controlled environment, such as by mimicking the features of a real-world arrangement such as a local area network connected to the security system. Thus, the security system of the present invention is arranged to perform one or more predetermined actions so that viruses present (for example, received within Internet traffic such as e-mails or other data) in the system preferably activate and execute actions that the security system is then able to detect as abnormal events likely caused by an unknown virus. In response to such detection, protective, corrective and proactive actions may be taken including transmitting alarms and closing/isolating infected connections, for example.

On the contrary, CHEFALAS et al. use traditional virus scanners for detecting virus fingerprints from the available data. Such approach requires having up-to-date virus information databases available and does not try to purposefully activate any virus as only monitoring of known viruses is provided.

It shall be noted that even if CHEFALAS et al. provided means, which they do not, for monitoring activation of previously unknown (thus, no fingerprint, i.e. characterizing code portion, available) viruses, such monitoring would be rather difficult to carry out as the solution would lack the presence of true excitation-response pairs that facilitates recognizing the activation of unknown viruses in the present invention. Namely, when the system of the present invention executes one or more predetermined actions for activating unknown viruses, it is easier, on the basis of the timing of such actions and the nature of such actions, to try to analyze events occurring afterwards whether they really relate to a virus activation or not. Meanwhile, it is much harder to estimate whether some event relates to virus activation if any actions for potentially triggering virus activations have not been recently taken.

In view of the present amendment and the foregoing remarks, it is believed that the present application has been placed in condition for allowance. Reconsideration and allowance are respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any

overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

Thomas W. Perkins, Reg. No. 33,027
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

TWP/lk